UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/585,317	07/06/2006	Paul Studerus	Q95553	2461

23373 7590 01/10/2008

SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

EXAMINER	
HSIEH, PING Y	

ART UNIT	PAPER NUMBER
2618	

MAIL DATE	DELIVERY MODE
01/10/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/585,317	STUDERUS, PAUL	
	Examiner	Art Unit	
	Ping Y. Hsieh	2618	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 July 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 July 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7/6/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims18-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claimed invention appears to be directed towards a computer program, which is not patentable eligible subject matter. Any computer executable software code must be stored in a computer readable storage medium to enable the underlying functionality. A structural and functional interrelationship between the computer program and the structural elements of the computer, which would permit its functionality to be realized, should be included in the claim. An example of acceptable language under 35 U.S.C. 101 would be "a computer readable medium storing a computer program...".

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 9-15 and 17-18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. Claims 9-15 and 17-18 provide for the use of an access control system, but, since the claim does not set forth any steps involved in the method/process, it is unclear what method/process applicant is intending to encompass. A claim is indefinite where it merely recites a use without any active, positive steps delimiting how this use is actually practiced.

Claims 9-15 and 17-18 are rejected under 35 U.S.C. 101 because the claimed recitation of a use, without setting forth any steps involved in the process, results in an improper definition of a process, i.e., results in a claim which is not a proper process claim under 35 U.S.C. 101. See for example *Ex parte Dunki*, 153 USPQ 678 (Bd.App. 1967) and *Clinical Products, Ltd.* v. *Brenner*, 255 F. Supp. 131, 149 USPQ 475 (D.D.C. 1966).

4. Claim 17 recites the limitation "time recording system" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claims 1-7 and 9-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Straumann et al. (U.S. PATENT NO. 7,196,610) in view of Kniffin et al. (U.S. PATENT NO. 6,072,402).

-Regarding claim 1, Straumann et al. disclose an access control system having a standard access control system **(as disclosed in fig. 1)**, via which a large number of access points can each be controlled via individual physical locking mechanisms **(access control device 1 is connected to an electromechanical lock 15; the access control system comprises a plurality of access control devices 1, 1' which control access doors 3, 3' as disclosed in fig. 1 and further disclosed in col. 5 lines 44-63)**, with at least one reader as well as a controllers, which is connected to it, for controlling the locking mechanisms being provided at each access points **(the access control device 1 further comprises an access control module 13 as disclosed in fig. 1 and further disclosed in col. 6 lines 25-47)**, characterized in that a short-range transmitter is provided at one specified location and transmits access-point-specific identification information in such a manner that this is received by a mobile telephone which is located in the reception area of the transmitter, and is used at least indirectly by this to control the access control at a specific associated access points **(the communication module 11 comprises a**

transceiver for wireless data communication by means of electromagnetic waves; the stored access control device identification is transmitted via the communication module 11 when the presence of an external communication terminal 2 is detected by the communication module 11 as disclosed in fig. 1 and further disclosed in col. 5 line 67-col. 6 line 18). However, Straumann et al. fail to disclose at least one access control server being provided, which carries out central management of the access data and is connected to the respective controllers; at least one mobile telephony server connected to the access control server, which is at least indirectly able to send data via a mobile telephone network to mobile telephone subscribers, and to receive data from them, in which case this mobile telephony server may also be an integral component of the access control server.

Kniffin et al. disclose at least one access control server being provided, which carries out central management of the access data and is connected to the respective controllers **(clearinghouse 54 transmits an RF signal to the identified lock and causes it to briefly make itself susceptible to being unlocked as disclosed in fig. 3 and further disclosed in col. 7 lines 20-30)**; at least one mobile telephony server connected to the access control server, which is at least indirectly able to send data via a mobile telephone network to mobile telephone subscribers, and to receive data from them, in which case this mobile telephony server may also be an integral component of the access control server **(RF transmission system is connected to the clearinghouse and**

receiving calls from the cellular telephone 52 as disclosed in fig. 3 and further disclosed in col. 7 lines 20-21).

Therefore, it would have been obvious to one of ordinary skills in the art at the time of invention to modify the access control device as disclosed by Straumann et al. to connect to an access control server (clearinghouse) as disclosed by Kniffin et al. One is motivated as such in order to provide a central monitoring system for improving security.

-Regarding claims 2 and 10, the combination further discloses the specified location is a location in the area of the associated access point, such that the identification information from the transmitter can be received by the mobile telephone only in the immediate vicinity of the access points **(Straumann et al., the communication module 11 is located in the area of the associated access point as disclosed in fig. 1 and the communication module 21 is activated by the user of the mobile communication terminal 2 in the vicinity of the access control device 1 to be passed as disclosed in col. 8 lines 14-16)**.

-Regarding claim 3, the combination further discloses the specified location is a location in front of the associated access points **(Straumann et al., as disclosed in fig. 1)**.

-Regarding claim 4, the combination further discloses the transmitter is a Bluetooth appliance **(Straumann et al., the communication module 11 comprises a Bluetooth transceiver for wireless data communication by**

means of electromagnetic waves as disclosed in col. 6 line 5), particularly preferably with a range of less than 10 meters **(it is inherent for the Bluetooth range to be less than 10 meters)**, and in that the authorized mobile telephone has a Bluetooth interface **(Straumann et al., the communication module 21 is corresponding to the communication module 11 for data exchange with the access control devices 1 as disclosed in col. 6 lines 62-65)**.

-Regarding claim 5, the combination of Straumann et al. and Kniffin et al. teaches all the limitations as claimed in claim 1. Straumann et al. disclose the communication module 11 comprises a transceiver for wireless data communication by means of electromagnetic waves in col. 6 lines 1-5 and the communication module 21 is corresponding to the communication module 11 for data exchange with the access control devices 1 as disclosed in col. 6 lines 62-65. Even thought the combination does not specifically disclose the interface is WLAN, it would have been obvious to one of ordinary skills in the art at the time of invention to modify the interface to be WLAN. One is motivated as such in order to provide for a cost efficient and ease of integration system.

-Regarding claim 6, the combination further discloses the identification information is a hardware-specific, unique address of the transmitter, particularly preferably an appliance-specific 48-bit address of a Bluetooth appliance **(it is inherent for each Bluetooth appliance to have a unique 48-bit address and use the address for connecting to other Bluetooth device)**.

-Regarding claim 7, the combination further discloses the transmitter is in the form of an independent unit, which preferably has no direct connection to the mobile telephony server **(Straumann et al., communication module 11 is not direct connected to the mobile telephony server as disclosed in fig. 1)**.

-Regarding claim 9, the combination further discloses a method for access control, particularly preferably using an access control system as claimed in claim 1, with a standard access control system being provided **(Straumann et al., as disclosed in fig. 1)**, via which a large number of access points can each be controlled via individual physical locking mechanisms **(Straumann et al., access control device 1 is connected to an electromechanical lock 15; the access control system comprises a plurality of access control devices 1, 1' which control access doors 3, 3' as disclosed in fig. 1 and further disclosed in col. 5 lines 44-63)**, with at least one reader as well as a controller, which is connected to it, preferably being provided in order to control the locking mechanism for each access points **(Straumann et al., the access control device 1 further comprises an access control module 13 as disclosed in fig. 1 and further disclosed in col. 6 lines 25-47)**, and with at least one access control server being provided, which carries out central management of the access data and is connected to the respective controllers **(Kniffin et al., clearinghouse 54 transmits an RF signal to the identified lock and causes it to briefly make itself susceptible to being unlocked as disclosed in fig. 3 and further disclosed in col. 7 lines 20-30)**; and with at least one mobile

telephony server being provided, connected to the access control server, which is at least indirectly able to send data via a mobile telephone network to mobile telephone subscribers, and to receive data from them, in which case this mobile telephony servers may also be an integral component of the access control server **(Kniffin et al., RF transmission system is connected to the clearinghouse and receiving calls from the cellular telephone 52 as disclosed in fig. 3 and further disclosed in col. 7 lines 20-21)**; characterized in that a short-range transmitter is provided with a specified location, preferably at least one access point **(Straumann et al., the communication module 11 is located in the area of the associated access point as disclosed in fig. 1)**, in that a mobile telephone is authorized for access at specific access points in a specific time period via the access control server **(Kniffin et al., after suitable verification, the clearinghouse transmits an RF signal to the identified lock and causes it to briefly make itself susceptible to being unlocked such as for 30 seconds as disclosed in col. 7 lines 22-25)**, in that the transmitter transmits access-point-specific identification information continuously or at times, in such a manner that it can be received by only a mobile telephone which is located in the reception area of the transmitter **(Straumann et al., the communication module 21 is activated by the user of the mobile communication terminal 2 in the vicinity of the access control device 1 to be passed as disclosed in col. 8 lines 14-16)**, in that a mobile telephone which is located in the reception area of the transmitter detects the identification of this

transmitter via this identification information **(it is inherent for each Bluetooth appliance to have a unique 48-bit address and use the address for connecting to other Bluetooth device when they are in range)**, and in that the access point associated with the transmitter is then opened, with direct or indirect use of this identification information, via the mobile telephone, the mobile telephone network, the mobile telephony server, the access control server and the controllers **(Kniffin et al., the user operates the cellular telephone 52 to call the clearing house 54 and request access to a particular lock 56 as disclosed in fig. 3 and further disclosed in col. 7 lines 20-22)**.

-Regarding claim 11, the combination further discloses after detection of the identification information **(Straumann et al., the communication module 21 is activated by the user of the mobile communication terminal 2 in the vicinity of the access control device 1 to be passed as disclosed in col. 8 lines 14-16)**, the mobile telephone additionally demands the input of an authentication in particular such as a PIN code and this user-specific information is transmitted together with the identification of the access point to be processed via the mobile telephone network to the mobile telephony server and to the access control server, which then activates the associated controller **(Kniffin et al., as disclosed in col. 2 lines 31-43)**.

-Regarding claims 12, 18 and 19, the combination further discloses the mobile telephone transmits the identification information and if appropriate the PIN code **(Kniffin et al., PIN number is provided by the user using a**

telephone's touch tone pad 22 as disclosed in col. 2 lines 42-43) via the GSM network in the form of a telephonic data transmission **(Straumann et al., the mobile radio network 5 is a GSM network as disclosed in col. 6 lines 58-61)**.

-Regarding claim 13, the combination further discloses the transmitter is a Bluetooth appliance **(Straumann et al., the communication module 11 comprises a Bluetooth transceiver for wireless data communication by means of electromagnetic waves as disclosed in col. 6 line 5)**, which transmits its unique address as identification information, and this address is used to identify the associated access point **(it is inherent for each Bluetooth appliance to have a unique 48-bit address and use the address for connecting to other Bluetooth device when they are in range)**, and in that the mobile telephone has a Bluetooth interface **(Straumann et al., the communication module 21 is corresponding to the communication module 11 for data exchange with the access control devices 1 as disclosed in col. 6 lines 62-65)**, in which case the mobile telephone automatically starts an appropriate dialogue with the mobile telephone user on reception of specific addresses of this type which are transmitted in the course of the authorization process and correspond to the authorized access points **(Kniffin et al., the user establishes communication to a clearinghouse 18, a series of voice prompts synthesized by a computer 20 at the clearinghouse and relayed to the user over the link 16 solicits the user to identify the lock 12 to which**

access is desire (the lock is usually identified by a number, in this case, the lock is identified by the Bluetooth address gathered by the communication module 21 as disclosed by Straumann et al.) as disclosed in col. 2 lines 31-40), possibly requests authentication of the user, and in any case then transmits a request to open the specific access point via the mobile telephone network to the mobile telephony server and to the access control server **(Kniffin et al., as disclosed in col. 2 lines 31-43)**.

-Regarding claim 14, the combination of Straumann et al. and Kniffin et al. teaches all the limitations as claimed in claim 1. Straumann et al. disclose the combination further discloses the transmitter is a Bluetooth appliance **(Straumann et al., the communication module 11 comprises a Bluetooth transceiver for wireless data communication by means of electromagnetic waves as disclosed in col. 6 line 5)**. Even thought the combination does not specifically disclose the transmitter is arranged in the area of the gateway in such a way that the identification information can be received by a mobile telephone only within a distance of less than 1 m, particularly preferably less than 0.5 m outside and in front of the gateway, it would have been obvious to one of ordinary skills in the art at the time of invention to do so. One is motivated as such in order to provide for power conservation by limiting the range of Bluetooth transmitter to 1 m.

-Regarding claim 15, the combination further discloses the transmitter is a Bluetooth appliance **(Straumann et al., the communication module 11**

comprises a Bluetooth transceiver for wireless data communication by means of electromagnetic waves as disclosed in col. 6 line 5), which is arranged in a specific area in front of the associated access point **(Straumann et al., the communication module 11 is located in the area of the associated access point as disclosed in fig. 1 and the communication module 21 is activated by the user of the mobile communication terminal 2 in the vicinity of the access control device 1 to be passed as disclosed in col. 8 lines 14-16)**.

-Regarding claim 16, Kniffin et al. disclose a access recording system having a standard access recording system which comprises at least one access recording server which carries out central management of the access data **(the secure access system to record data relating to lock access as disclosed in col. 4 lines 52-53 and the access log data is RF-transmitted to the clearinghouse as disclosed in col. 5 lines 3-4)**; at least one mobile telephony server in conjunction with the access recording server, which is at least indirectly able to transmit data via a mobile telephone network to mobile telephone subscribers, in which case this mobile telephony server may also be an integral component of the time recording server **(RF transmission system is connected to the clearinghouse and receiving calls from the cellular telephone 52 as disclosed in fig. 3 and further disclosed in col. 7 lines 20-21)**; and a proximity detector **(as disclosed in col. 3 lines 50-63).** However, Kniffin et al. does not specifically point out the access data comprises time data and the proximity

detector is a short-range transmitter is provided for at least one authorized areas and transmits area-specific identification information in such a way that it is received only by a mobile telephone which is located in the immediate vicinity of the authorized area, and is used by this mobile telephone at least indirectly for the manipulation of the time data.

Straumann et al. disclose time determination module 14 for determining current time indications; and a short-range transmitter **(the communication module 11 comprises a Bluetooth transceiver for wireless data communication by means of electromagnetic waves as disclosed in col. 6 line 5)** is provided for at least one authorized areas and transmits area-specific identification information in such a way that it is received only by a mobile telephone which is located in the immediate vicinity of the authorized area **(the communication module 11 is located in the area of the associated access point as disclosed in fig. 1 and the communication module 21 is activated by the user of the mobile communication terminal 2 in the vicinity of the access control device 1 to be passed as disclosed in col. 8 lines 14-16)**, and is used by this mobile telephone at least indirectly for the manipulation of the time data **(the communication module 21 is activated by the user of the mobile communication terminal 2 in the vicinity of the access control device 1 to be passed as disclosed in col. 8 lines 14-16)**.

Therefore, it would have been obvious to one of ordinary skills in the art at the time of invention to modify the access data as disclosed by Kniffin et al. to

include the time data as disclosed by Straumann et al. One is motivated as such in order to provide a complete access data log for improving the security record. It would have been obvious to one of ordinary skills in the art at the time of invention to further modify the proximity detector as disclosed by Kniffin et al. to be a short-range transmitter as disclosed by Straumann et al. One is motivated as such in order to provide for power conservation by using a low power transmitter such as Bluetooth transmitter.

-Regarding claim 17, the combination further discloses a standard time recording system which comprises at least one time recording server carrying out central management of the time data **(Kniffin et al., the secure access system to record data relating to lock access as disclosed in col. 4 lines 52-53 and the access log data is RF-transmitted to the clearinghouse as disclosed in col. 5 lines 3-4)**, and with at least one mobile telephony server in conjunction with the time recording server, which is at least indirectly able to transmit data via a mobile telephone network to mobile telephone subscribers, in which case this mobile telephony servers may also be an integral component of the time recording server **(Kniffin et al., RF transmission system is connected to the clearinghouse and receiving calls from the cellular telephone 52 as disclosed in fig. 3 and further disclosed in col. 7 lines 20-21)**; in that a short-range transmitter is provided for at least one authorized area, characterized in that a mobile telephone is authorized to input time data in specific authorized areas, in at least one specific time period, via the time recording server and via

the mobile telephony server via the mobile telephone network **(Straumann et al., stored, assigned in each case to the access control device identification for an access control device 1, in the data store of the access authorization module 221 are the access code for the respective access control device 1 and access rights data, which define time periods during which the user can be granted access to the object controlled by the respective access control device 1 as disclosed in col. 7 lines 9-30)**, in that the transmitter transmits area-specific identification information continuously or at times, in such a manner that it can received only by a mobile telephone which is located in the immediate vicinity of the authorized area **(Straumann et al., the communication module 11 is located in the area of the associated access point as disclosed in fig. 1 and the communication module 21 is activated by the user of the mobile communication terminal 2 in the vicinity of the access control device 1 to be passed as disclosed in col. 8 lines 14-16)**, in that a mobile telephone which is located in the immediate vicinity of the area detects the identification of this area via this identification information **(it is inherent for each Bluetooth appliance to have a unique 48-bit address and use the address for connecting to other Bluetooth device)**, and in that time data is then transmitted to the time recording server, and/or is checked by the latter, via the mobile telephone, the mobile telephone network and the mobile telephony server **(Kniffin et al., the user operates the cellular telephone 52 to**

call the clearing house 54 and request access to a particular lock 56 as disclosed in fig. 3 and further disclosed in col. 7 lines 20-22).

4. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Straumann et al. (U.S. PATENT NO. 7,196,610) in view of Kniffin et al. (U.S. PATENT NO. 6,072,402) and further in view of Want et al. (U.S. PG-PUB NO. 2003/0114104).

-Regarding claim 8, the combination of Straumann et al. and Kniffin et al. teaches all the limitations as claimed in claim 1. Straumann et al. disclose the communication module 11 comprises a transceiver for wireless data communication by means of electromagnetic waves in col. 6 lines 1-5 and the communication module 21 is corresponding to the communication module 11 for data exchange with the access control devices 1 as disclosed in col. 6 lines 62-65. However, the combination fails to disclose characterized in that the standard access control system also allows access control using means without mobile telephony, in particular based on RFID technology.

Want et al. disclose each portable electronic device 14, 16, 18 includes a radio frequency identification (RFID) tag 24 and, accordingly, the computer access device 12 includes a complimentary RFID reader 26 as disclosed in fig. 1 and paragraph 11.

Therefore, it would have been obvious to one of ordinary skills in the art at the time of invention to modify the interface to be RFID. One is motivated as such in order to provide for ease of operating the system.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Rodenbeck et al. (U.S. PATENT NO. 6,720,861) and Nielsen (U.S PG-PUB NO. 2002/0180582).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ping Y. Hsieh whose telephone number is 571-270-3011. The examiner can normally be reached on Monday-Thursday (alternate Fridays) 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lana Le can be reached on 571-272-7891. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

PH

1-05-08

LANA LE
PRIMARY EXAMINER